



# **US Department of Energy**

## **Albuquerque Operations Office**

### **20th DOE Computer Security Group Training Conference**



# Computer Virus Protection Workshop

## Albuquerque's Version of the Story

Gordon Besson, CISSP



# Background

- NT 3.5.1 on servers, Win3.x and WFW on workstations
- Transition to NT client on all WS
- F-Prot virus checker for WS, none for servers
- Evaluating many virus checkers: McAfee, Norton, Inoculan, Dr Solomon, Norman, many others

# Background (cont'd)

- NT on WS w/ only F-Prot allowed macro viruses to leave DOE/AL
- MANY macro viruses went to HQ!
- ASSIST report - Albuq accounted for 60% of HQ viruses in 3rd Qtr '97!
- After implementation, viruses sent to HQ dropped to 7 (Aug + Sep)

# Present Operating Environment

- Approx 1,700 workstations. 1,200 networked using Win NT 3.5.1 client
- Stand-alones w/ NT, Win 3.x, DOS
- 98% now migrated to Win NT client
- 30 servers, medium to high-end
- MS Exchange
- FY98 - migrate to Windows NT 4.0

# Protections

- Workstations
  - Inoculan and Dr. Solomon
- Servers
  - Inoculan
- Firewall
  - none

# Virus Reporting Procedures

- Users call Helpline for all computer problems/assistance, etc
- If call is virus-related, forwarded to Computer Security Group, or Computer Technicians staff

# Virus Incident Response Procedures

- Helpline, CSG or Techs will render assistance
- If a new virus, or unrecognized - CSG notified, CIAC notified immediately
- Users assisted in eradication
- Techs dispatched if user unable to eradicate

# Install/Update Process (2)

- Servers and networked workstations automatically updated with Inoculan, using SMS
- Stand-alone, laptop and home-use users are notified that a new version of Dr Solomon on the server
  - Classified users update via diskettes
  - Unclassified users download or dial-up

# Auditing

- Inoculan provides extensive, daily reports.
- SMS tells which workstations have Inoculan installed

# Data/Report Collection

- Inoculan provides activity reports for networked workstations
- No reporting for stand-alones or laptops

# Lessons Learned

- **DON'T INFECT HQ!!**
- **Recommend at least 2 virus checkers per site. If one fails, or reports no detail, 2nd checker may identify/catch the virus. This has happened to DOE/AL-twice!**
- **Major configuration changes - get your virus checking act together well in advance!**

# User Education Initiatives

- Broadcast messages - users informed of a new 'transparent' virus checking activity to scan their C: drives at 11:30 am every day
- Broadcast message - informs users of the latest version of Dr. Solomon for them to download

# Support Staff Education

- Helpline, Techs and CS Group that work w/ virus incidents are trained periodically
- Timely notification of viruses, hoaxes and chain letters, per CIAC bulletins/notices

# Collaborative Education Initiatives

- Contractors are mandated by their contracts to install/use virus checkers on their company-supplied systems on DOE/AL premises

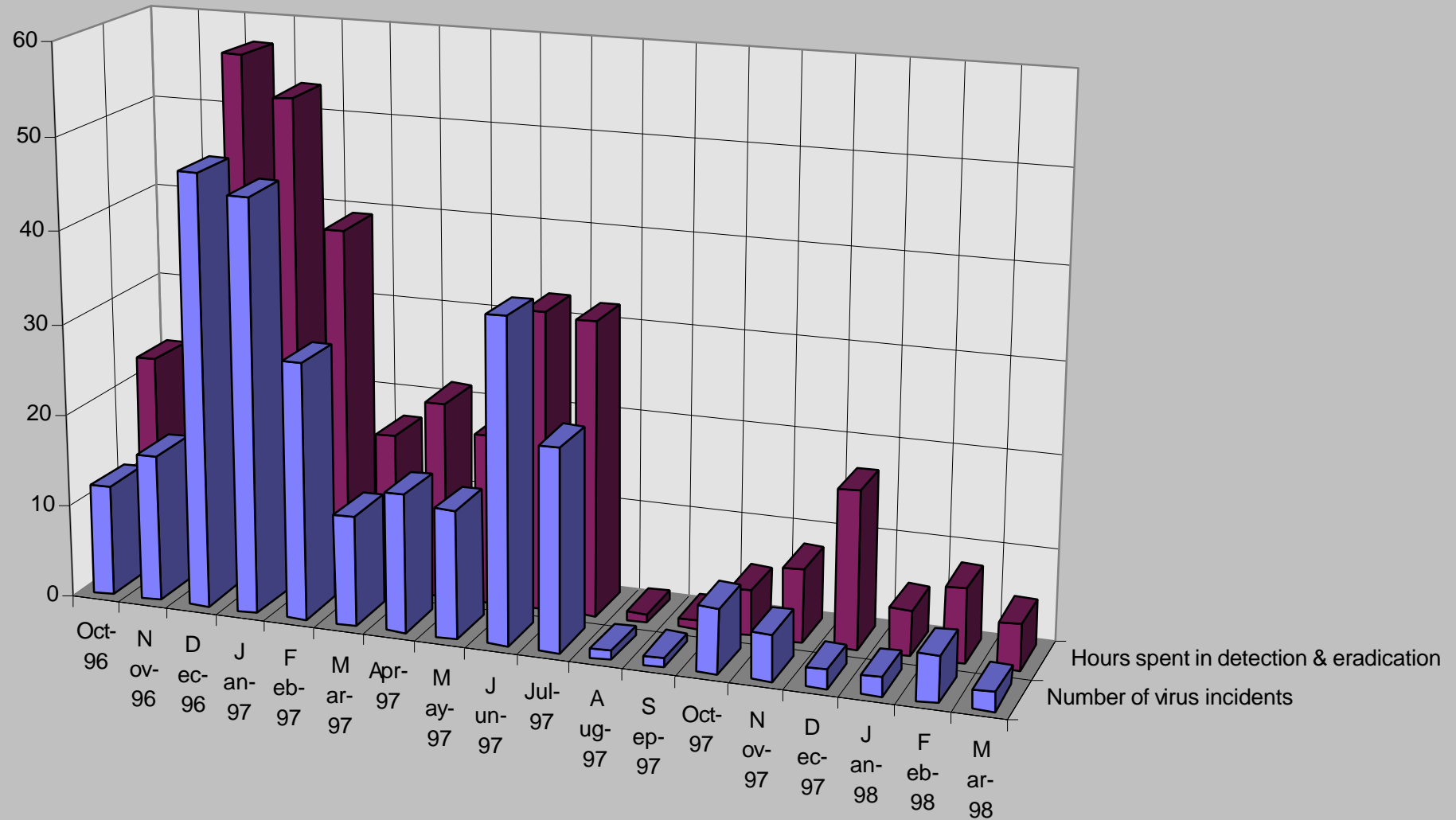
# Virus Support Staff Resources

- 1-2 persons on Helpline
- 2-3 Computer Technicians
- 1 person in CS Group
- Above are 'experts'. Others w/ less experience are also available.

# Costs

- Inoculan - \$27,800 for 2-yr license for 1,750 workstations and 30 servers
- Dr Solomon - \$22,800 for 2-yr license for 2,000 workstations
- F-Prot - \$500 for 1-yr license for use by some users

# Virus Statistics History



# More Statistics

## ■ Before virus checkers:

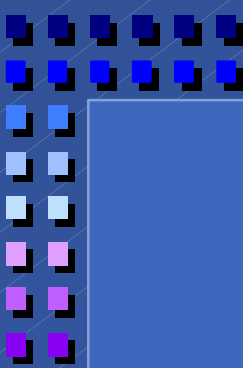
- ‘Blue Screen of Death’ 10-20 / week
- 10-50 infected files / server / day
  - » most was 66 files on one workstation!

## ■ After virus checkers:

- No ‘Blue Screens’ yet
- 1-3 infected files / server / week
- Some infected email mssgs; but cleaned immediately

# Some More Statistics

- Converting workstation hard drives from FAT to NTFS has virtually eliminated our boot virus problem
- Biggest vulnerability now is viruses on diskettes brought into the facility
- Another vulnerability is old files being 'attached' to documents without opening them first. Opening allows Inoculan to cleanse them



And now you  
know our side  
of the story!!

